BakerHostetler

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

May 21, 2024

United States District Judge Edgardo Ramos
United States District Court for the Southern District of New York
40 Foley Square, Courtroom 619
New York, NY 10007

Re: Gabrielli v. Insider, Inc. -- 1:24-cv-01566-ER

Dear Judge Ramos:

We represent Insider, Inc. ("Business Insider") in the above-referenced matter. We write to request a pre-motion conference seeking permission to file a motion to dismiss Plaintiff Jonathan Gabrielli's ("Plaintiff") Class Action Complaint (the "Complaint") under Fed. R. Civ. P. 12(b)(1) and 12(b)(6).

I. PLAINTIFF'S ALLEGATIONS

Plaintiff's allegations are: (1) through its website, www.businessinsider.com, Business Insider installs a "tracker" on the browser of each individual who visits the website, which in turn captures and sends to Audiencerate—the developer of the tracker—the visitor's IP address, [Dkt. No. 1, ¶¶ 1-2, 22, 26-27]; (2) "[b]ecause the Audiencerate Tracker captures outgoing information—the IP address—from visitors to" www.businessinsider.com, the tracker "is a 'pen register' for purposes" of California Invasion of Privacy Act ("CIPA") § 638.50(b), [*id.* at ¶ 38]; and (3) because CIPA makes it unlawful to install or use a pen register absent a court order, which Business Insider did not obtain, Business Insider violated CIPA and, in turn, is subject to $5,000 in statutory penalties per violation, [*id.* at ¶¶ 71-72, 74-76].

II. PEN REGISTERS AND THE SURGE IN PEN-REGISTER CLASS ACTIONS

CIPA defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b). Historically, pen registers were used by law enforcement personnel to identify the telephone numbers that were being dialed by a person of interest in a criminal investigation. *See Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) ("Traditionally, law enforcement used 'pen registers' in investigations to record all numbers called from a particular telephone[.]"). In that scenario, law enforcement could see which telephone numbers were being dialed *despite not being a party to the conversation*.

With the rise of the internet, the use of pen registers has expanded beyond telephone lines, to include email and website browsing. *United States v. Forrester*, 512 F.3d 500, 504 (9th Cir. 2008). Regardless of the medium (telephone or internet), however, one thing remains true: pen registers are installed and used by parties ***not involved in the conversation*** in order to identify the parties to the conversation. Even in *Greenley*., 684 F. Supp. 3d 1024, the case giving rise to these suits and cited by Plaintiff in the Complaint, the party installing the pen register was an unknown third party. There, the plaintiff installed on his phone applications that were developed by companies that used the defendant's "software development kit ('SDK')." *Id.* at 1035. The defendant, a "data broker," allowed these

companies to use its SDK in exchange for them "allow[ing] Defendant to 'surreptitiously intercept location data' from" their app users. *Id.* The plaintiff claimed that the defendant, with whom the plaintiff had not interacted, unlawfully installed a "pen register." *Id.* at 1036. The court agreed. *Id.* at 1051.

Throughout its opinion, the *Greenley* court focused on the surreptitious nature of the defendant's conduct. *Id.* at 1050 (noting that CIPA's pen-register statute could apply to non-law enforcement entities because "private companies and persons have the ability to ***hack*** into a person's telephone and gather the same information as law enforcement" and rejecting "the contention that a private company's ***surreptitiously*** embedded software installed in a telephone cannot constitute a 'pen register'"(emphasis added).).

The holding in *Greenley* is neither surprising nor novel. In *Greenley*, a third party, unknown to the individual (traditionally, law enforcement and, in *Greenley*, the defendant), surreptitiously gathered information about the individual that, without the use of the pen register, it would not have had access to (dialed telephone numbers for law enforcement and location data in *Greenley*).

Despite the straightforward nature of *Greenley*, plaintiffs have, for the last year, interpreted it to mean that a company with whom an individual affirmatively interacts (i.e., visits the company's website) and to whom the individual voluntarily provides his or her IP address (a necessary requirement to visit any website) unlawfully uses a 'pen register' by capturing his or her IP address. That is wrong.

III. WHY PLAINTIFF'S CLAIM FAILS

Plaintiff's Complaint suffers from several fatal flaws. As a threshold issue, Plaintiff has not alleged sufficient facts to establish that he has suffered an injury-in-fact for purposes of Article III standing. Even if he had, he still has not alleged sufficient facts to establish that anything Business Insider did on its own website violated CIPA.

A. Plaintiff Has Suffered No Injury-In-Fact.

The law is clear: "Those who do not possess Art. III standing may not litigate as suitors in the courts of the United States." *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 475–76 (1982). Standing requires the plaintiff to have, among other things, " suffered an injury in fact[.]" *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016), *as revised* (May 24, 2016). Plaintiff has not alleged and cannot allege an injury-in-fact.

To establish injury-in-fact, "a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id.* at 339 (internal quotations omitted). Concrete injuries can be "tangible" (i.e., "physical harms and monetary harms") or they can be "intangible." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021). Plaintiff does not and cannot allege that he suffered any "tangible" harms from Insider's conduct. [*See generally* Dkt. No. 1.] He, therefore, must allege an "intangible" harm.

Intangible harms do not arise simply because the plaintiff alleges that the defendant violated a statute. *TransUnion LLC*, 594 U.S. at 427 ("[U]nder Article III, an injury in law is not an injury in fact."). Instead, they require "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," like "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* at 425.

Here, Plaintiff claims that he "had his privacy invaded by Defendant's violations of CIPA § 638.51(a)." [Dkt. No. 1.] That is not true. As an initial matter, "there is no common-law right of action for invasion of privacy" under New York law. *Mills v. Miteq, Inc.*, No. CV06-752(SJF)(AKT), 2007 WL 2908218, at

*5 (E.D.N.Y. Sept. 14, 2007), *report and recommendation adopted*, No. 06-CV-0752 (SJF), 2007 WL 2932816 (E.D.N.Y. Oct. 3, 2007). Instead, under New York law, an invasion of privacy claim is exclusively statutory and only arises "when one's name, likeness or voice has been used for advertising purposes or in commerce without permission," *id.*, which Plaintiff does not allege, [*see generally* Dkt. No. 1.] But even beyond New York law, any invasion-of-privacy theory requires the plaintiff to establish a "reasonable expectation of privacy" in the information allegedly collected or disclosed. *Weisshaus v. Cuomo*, 512 F. Supp. 3d 379, 393 (E.D.N.Y. 2021).

The only information that Plaintiff alleges Business Insider collected and/or disclosed is his IP address. [Dkt. No. 1, ¶¶ 2, 45.] IP addresses have long been held not to be private in nature because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *see also United States v. Kidd,* 394 F. Supp. 3d 357, 362 (S.D.N.Y. 2019) ("[M]ost courts have adopted a categorical approach holding that users have no reasonable expectation of privacy in such IP address information.").

This case is no different. By visiting www.businessinsider.com, Plaintiff voluntarily provided his IP address to Business Insider. Plaintiff, therefore, has no reasonable expectation of privacy in his IP address and has failed to establish an intangible, concrete harm sufficient for Article III standing. *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1190 (N.D. Cal. 2020) (holding that plaintiffs "cannot be injured from the collection of IP addresses, and so lack Article III standing for the privacy claims").

B. Plaintiff Has Not Alleged a Violation of CIPA.[1]

Admittedly, what constitutes a pen register has largely gone unlitigated, given that, in most instances, courts are asked to permit the use of a pen register, not to determine whether one is being used in the first place. That said, courts that have considered whether tracking technologies utilized on a publicly accessible website are pen registers have found that they are not.

In *Licea v. Hickory Farms LLC*, No. 23STCV26148, 2024 WL 1698147 (Cal.Super. Mar. 13, 2024), a California trial court found that such tracking technologies were not pen registers under CIPA because, among other things, (1) the plaintiff "voluntarily disclosed" his IP address to the defendant, (2) an IP address alone is not "qualifying information for the establishment of a violation," and (3) the plaintiff's interpretation of "pen registers" would make "every single entity" whose website a plaintiff "voluntarily visited" "a violator" of the statute. *Id.* at *4.

One month later, the same California court reached the same conclusion. *Casillas v. Transitions Optical, Inc. Case* No. 23STCV30742 (Cal. Super. Ct. L.A. Cnty. April 23, 2024). In doing so, the court found the plaintiffs' reliance on *Greenley* "unpersuasive" because "the alleged conduct and relationship to the plaintiff" in *Greenley* (i.e., an unknown third party surreptitiously collecting an unsuspecting individual's location data) "was very different from the allegations here" (i.e., the operator of a website voluntarily visited by plaintiff collecting the IP address that he voluntarily provided). *Id.*

In truth, while no court has affirmatively specified the elements necessary to state a pen-register claim under CIPA, case law makes clear that the plaintiff must allege, at the very least, (1) that the information being collected was something more than just an IP address and (2) that the entity doing the collecting was not the party with whom the plaintiff was interacting. Plaintiff has failed to state a violation of CIPA; his complaint must be dismissed.

---

[1] Plaintiff has likewise fails to allege sufficient facts to establish that CIPA applies to Insider at all, given that CIPA does not apply extraterritorially, and Plaintiff has not alleged that any of the acts complained of in the Complaint occurred within California's borders.

Respectfully submitted,

/s/ Robyn M. Feldstein

Robyn M. Feldstein
cc: All Plaintiffs' Counsel (via ECF)